# Security of EPR-based Quantum Key Distribution

Hitoshi Inamori
Centre for Quantum Computation, Oxford University

February 1, 2008

**Abstract**

We propose a proof of the security of EPR-based quantum key distribution against enemies with unlimited computational power. The proof holds for a protocol using interactive error-reconciliation scheme. We assume in this paper that the legitimate parties receive a given number of single photon signals and that their measurement devices are perfect.

## 1 Introduction

Quantum key distribution is a cryptographic task that uses properties of quantum mechanics to allow two legitimate parties to share a secret random number. This random number can be used as a key for a symmetric classical cipher to establish a perfectly secure communication channel between the legitimate parties. The first quantum key distribution protocol, called BB84, was proposed by Bennett and Brassard [1]. It was followed by other protocols, such as [2, 3] and the security of these protocols were analysed [4, 5, 6, 7, 8, 9, 10, 11]. The unconditional security of quantum key distribution – i.e. security against enemies with unlimited computational power – was obtained by Mayers [12, 13] for the BB84 protocol and many notions and techniques introduced in the proof are used in the present paper. Other proofs of the unconditional security of BB84 followed [14, 15, 16, 17, 18]. The security of EPR-based quantum key distribution protocol proposed by Ekert, E91 [3, 19], has also been proved in [14, 15, 17, 20], and the security of entanglement-based quantum key distribution using untrusted apparatus has been proved in [21, 22]. In this paper, we propose another proof of the security of E91. The protocol is proved secure against enemies with unlimited computational power. However, it is assumed that both legitimate parties receive an ensemble of a given number of single photons. Furthermore we assume that the efficiency of their detection unit is one, which is far from true in any practical implementation of quantum key distribution today. The results in this paper therefore do not apply to practical implementations of EPR-based quantum key distribution. Nevertheless it is hoped that techniques employed in this paper can be generalised to prove security of practical EPR-based quantum key distribution protocols.

## 2 Definition of security

We adopt the same definition of security as described in [13, 23].

The rôle of key distribution between two distant legitimate parties, traditionally called Alice and Bob, is to generate a shared random number, called the *private key*, that is guaranteed to be known only by the legitimate parties. A non-authorised party, traditionally called Eve, should not be able to obtain any information about the private key, whichever eavesdropping strategy she might adopt.

However, most quantum key distribution protocols do not allow Alice and Bob to share a private key in all circumstances. It is only when some conditions are satisfied that Alice and Bob can ascertain a potential eavesdropper will only have negligible information about the key. The protocol therefore provides a *validation test* that tells whether a key can be generated with unconditional privacy. A key is created only if the test is passed. Otherwise the session is abandoned. Nevertheless, as in [13, 23] we will adopt the convention that when the validation test is not passed, Alice chooses a random value for the private key with uniform probability distribution. As a result, the private key is defined regardless the outcome of the validation test, but, of course, when the validation test is not passed, Bob does not share the key with Alice.

Finally, we consider families of protocols for which a parameter quantifying the amount of a resource used in a protocol characterises its security. Such parameter is called *security parameter*. Usually, the higher the security parameter's value is, the higher is the level of security, but also the amount of a resource required by the protocol. We now give a formal definition of security.

A random variable will always be denoted by a bold letter, and values taken by this random variable by the corresponding plain letter. Only discrete random variables will be considered in this paper. The probability distribution of a random variable $\boldsymbol{x}$ is denoted by $\mathrm{P}_{\boldsymbol{x}}$, i.e. $\mathrm{P}_{\boldsymbol{x}}(x) = \Pr(\boldsymbol{x} = x)$ is the probability that $\boldsymbol{x}$ takes the value $x$. The joint distribution of two random variables $\boldsymbol{x}$ and $\boldsymbol{y}$ is denoted by $\mathrm{P}_{\boldsymbol{xy}}$, i.e. $\mathrm{P}_{\boldsymbol{xy}}(x, y) = \Pr(\boldsymbol{x} = x, \boldsymbol{y} = y)$. The conditional probability of $\boldsymbol{x}$ given that $\boldsymbol{y}$ takes a value $y$ is denoted by $\mathrm{P}_{\boldsymbol{x}\,|\,\boldsymbol{y}=y}$ whenever $\mathrm{P}_{\boldsymbol{y}}(y) > 0$, i.e. $\mathrm{P}_{\boldsymbol{x}\,|\,\boldsymbol{y}=y}(x) = \Pr(\boldsymbol{x} = x|\boldsymbol{y} = y) = \frac{\mathrm{P}_{\boldsymbol{xy}}(x,y)}{\mathrm{P}_{\boldsymbol{y}}(y)}$, whenever $\mathrm{P}_{\boldsymbol{y}}(y)$ is positive. Let $f$ be a function defined on the image of $\boldsymbol{x}$. When no confusion is possible, the notation $\boldsymbol{f}$ will be adopted to denote the random variable $f(\boldsymbol{x})$.

We will denote by $\vec{\boldsymbol{\kappa}}$ the random variable giving the private key generated in a key distribution session. The key is a string of $m$ bits where $m$ is a positive integer specified by the legitimate users. That is $\vec{\boldsymbol{\kappa}}$ takes value in $\{0,1\}^m$. Given an eavesdropping strategy chosen by Eve, we denote by $\boldsymbol{v}$ the random variable giving collectively all data Eve gets during this key distribution session. Henceforth, given the eavesdropping strategy adopted by Eve, $\boldsymbol{v}$ is called the *view* of Eve, and we will denote by $\mathcal{V}$ the set of all values $\boldsymbol{v}$ may take.

We adopt the following definition of security for quantum key distribution protocols.

**Definition 1** *Consider a quantum key distribution protocol returning a key $\vec{\boldsymbol{\kappa}} \in \{0,1\}^m$ regardless the outcome of the validation test, where the length of the key, $m$, is fixed and chosen by the user. We say that the protocol offers* perfect privacy *if and only if:*

- *the protocol is parametrised by a parameter $N$ taking value in $\mathbf{N}$ called the security parameter, and*
- *there exists a function $\epsilon : \mathbf{N} \times \mathbf{N} \to \mathbf{R}^+$ such that $\epsilon(N, m)$ is vanishing exponentially as $N$ grows (i.e. there exist $\alpha > 0$, $\beta > 0$, $N_{min} \in \mathbf{N}$ and a function $f : \mathbf{N} \to \mathbf{R}^+$ such that $\forall N > N_{min}$, $\epsilon(N, m) < e^{-\alpha N^\beta} f(m)$) , and*
- *there exists a function $N_0 : \mathbf{N} \to \mathbf{N}$ such that, for any strategy adopted by Eve,*

$$\begin{aligned} &\forall m, \forall N \geq N_0(m), \\ &\quad H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - \epsilon(N, m) \end{aligned}$$

*where $\boldsymbol{v}$ is Eve's view given her strategy, and*

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \stackrel{Def}{=} - \sum_{\vec{\kappa}, v \,:\, \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa}, v) > 0} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa}, v) \log_2 \mathrm{P}_{\vec{\boldsymbol{\kappa}} \,|\, \boldsymbol{v}=v}(\vec{\kappa})$$

*is the Shannon entropy [24, 25, 26] of the key $\vec{\boldsymbol{\kappa}}$ given Eve's view $\boldsymbol{v}$.*

Another important aspect of security of key distribution protocols is the *integrity* or the faithfulness of the distributed key. We must require that whatever Eve does, it is very unlikely that Alice and Bob fail to share an identical private key while the validation test is passed. However, the integrity of the protocol depends mainly on the efficiency of the error detection/correction scheme that is used. This point is discussed in Appendix, but the reader is referred for instance to [27] for a more complete explanation.

# 3 The protocol

We describe the quantum key distribution protocol under consideration. It is a variation [19] of the protocol originally proposed in [3]. The protocol is designed to use classical error-reconciliation schemes like the interactive scheme proposed in [27].

**Protocol setup**

Alice and Bob specify:

- $m$, the length (in bits) of the private key to be generated.
- $\epsilon$, the maximum threshold value for the error rate during the quantum transmission ($\epsilon < 1/4$).
- $\tau$, a security constant such that $\frac{2\epsilon}{1-\epsilon} < \frac{2\epsilon}{1-\epsilon} + \tau < 1$.
- the security parameter $r$. It must be large enough so that Alice and Bob can find a binary matrix $K$ of size $m \times r$ such that any linear combination of rows of $K$ that contains at least one row of $K$ has weight greater than $d_K = \left(2\frac{\epsilon}{1-\epsilon} + \tau\right) r$ (i.e. $\min_{\vec{x} \in \{0,1\}^m \setminus \vec{0}}(w(\vec{x}^T K)) \geq d_K$ where for any vector $\vec{y}$, $w(\vec{y})$ is the weight of $\vec{y}$, that is, the number

of non zero entries in $\vec{y}$). Alice and Bob choose one such matrix $K$. Shannon's coding theorem [25] tells that for asymptotic values of $m$, such matrix can be found if $r$ obeys the inequality:

$$\frac{m}{r} \leq 1 - h\left(\frac{\epsilon}{1-\epsilon} + \frac{\tau}{2}\right),$$

where $h(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)$ is Shannon's binary entropy.

- An error reconciliation scheme between Alice and Bob such that:
  - it tells, with high probability of correctness, whether more than $\epsilon s$ errors are present in a string of $s$ bits, where $s = \left\lfloor \frac{r}{1-\epsilon} \right\rfloor$,
  - if there are less than $\epsilon s$ errors in the string, the scheme corrects these errors, at least with high probability of success,
  - only positions of the errors are possibly disclosed publicly. In particular the scheme should disclose no information about parities of the reconciled string.

  The error reconciliation can be a probabilistic scheme for which an upper-bound on the probability of failure can be specified by Alice and Bob. One can achieve such a task by first estimating the error rate on a small randomly chosen proportion of the string and then by using for instance the interactive error-reconciliation scheme proposed in [27]. In these processes, the exchanged parities or bits should be encrypted with the one-time pad method [7, 10]. A basic explanation of this scheme can be found in Appendix A, but the reader is referred to [27] for a complete description. The above requires that Alice and Bob share beforehand a secret private key for the one-time pad encryption. According to Shannon's coding theorem, for asymptotic values of $s$, such probabilistic error-reconciliation is possible if the entropy[1] $q$ (in bits) of the previously shared private key obeys the inequality:

$$q \geq sh(\epsilon).$$

- $n$, the number of pairs of photons to be sent to the legitimate parties. A good choice for $n$ is $\left\lceil \frac{r}{\frac{1-\epsilon}{2} - \tau_S} \right\rceil$ where $\tau_S$ is a small but strictly positive constant.

**Quantum transmission**

- A source sends a sequence of $n$ photons to Alice and another sequence of $n$ photons to Bob. It is assumed that ideally, for each $i \in \{1 \ldots n\}$, the source emits a pair of photons in the state:

$$|\Phi^+\rangle = \frac{|0\rangle_+|0\rangle_+ + |1\rangle_+|1\rangle_+}{\sqrt{2}}$$

  and that Alice's $i$-th photon is the first photon of this pair, and Bob's $i$-th photon is the second photon of this pair. The kets $|0\rangle_+$ and

[1] That is, the length of the previously shared key if it is uniformly distributed.

$|1\rangle_+$ form an orthonormal basis + of the Hilbert space describing the polarisation of one photon. The kets $|0\rangle_\times = \frac{|0\rangle_+ + |1\rangle_+}{\sqrt{2}}$ and $|1\rangle_\times = \frac{|0\rangle_+ - |1\rangle_+}{\sqrt{2}}$ form its conjugate basis $\times$.

However, the source needs not to be trusted. In particular, it can be under control of a possible eavesdropper. The only assumption is that Alice and Bob receive a sequence of $n$ single photon signals on each side.

- We assume that the measurement devices of Alice and Bob have efficiency one. For each $i \in \{1 \dots n\}$,
  1. Alice picks randomly a basis $a_i \in \{+, \times\}$ with uniform probability distribution. Alice measures her $i$-th photon in the basis $a_i$, obtaining the outcome $\alpha_i \in \{0, 1\}$, corresponding to the state $|\alpha_i\rangle_{a_i}$.
  2. Similarly, Bob picks randomly and independently of Alice a basis $b_i \in \{+, \times\}$ with uniform probability distribution. Bob measures his $i$-th photon in the basis $b_i$, obtaining the outcome $\beta_i \in \{0, 1\}$, corresponding to the state $|\beta_i\rangle_{b_i}$.

**Sifting**

We denote by $\vec{a} = (a_1, a_2, \dots, a_n)$, $\vec{b} = (b_1, b_2, \dots, b_n)$, $\vec{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\vec{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$ the outcomes of the quantum transmission. For any vector $\vec{y} = (y_1, y_2, \dots, y_n)$ in $\{0, 1\}^n$ or $\{+, \times\}^n$, and for any subset $X$ of $\{1 \dots n\}$, we denote by $y_X$ the restriction of $\vec{y}$ on $X$.

Alice and Bob compare publicly their bases $\vec{a}$ and $\vec{b}$. We denote by $\vec{d}$ the vector in $\{0, 1\}^n$ such that for any $i \in \{1 \dots n\}$, $d_i = 1$ if and only if $a_i = b_i$. If the number of indexes $i \in \{1 \dots n\}$ such that $a_i = b_i$ is greater than or equal to $s$ (i.e. $w(\vec{d}) \geq s$) then the *sifted set* $S$ is defined as the set of the first $s$ such indexes. Otherwise the validation test is failed. The bit strings $\alpha_S$ and $\beta_S$ are usually referred to as the *sifted keys*.

**Error correction**

Alice and Bob perform the error correction on their sifted keys $\alpha_S$ and $\beta_S$ as specified in the protocol setup. We define the *error set* $E$ as the set of indexes in $S$ in which an error is found, that is, $\alpha_i \neq \beta_i$. Likewise, we define the *error vector* $\vec{e}$ as the vector in $\{0, 1\}^s$ giving the positions of the errors ($\forall i \in \{1, \dots, s\}$, $e_i = 1$ if and only if $\alpha_i \neq \beta_i$). We denote by $e$ the size of the set $E$, i.e. $e = |E| = w(\vec{e})$. The validation test is passed if $e < \epsilon s$, otherwise it is failed. If the validation test is passed, then Alice and Bob define the *reconciled set* $R$ as the set of the first $r$ indexes $i \in S \setminus E$ [2]. Therefore $|R| = r$ and $\forall i \in R$, $a_i = b_i$ and $\alpha_i = \beta_i$. Alice and Bob obtain an identical string of bits $\alpha_R \in \{0, 1\}^r$, called the *reconciled key*.

**Privacy amplification**

The private key is defined as:

1. $\vec{\kappa} = K\alpha_R \pmod 2$ if the validation test is passed.

[2] Note that $|S \setminus E| \geq r$ if the validation test is passed.

2. an $m$-bit string $\vec{\kappa}$ picked randomly by Alice with uniform probability distribution each time the validation test is failed.

# 4 Privacy of the protocol

The main result of this paper is stated.

**Property 1** *The protocol described above offers perfect privacy: for any eavesdropping strategy chosen by a possible eavesdropper, the conditional entropy of the private key $\vec{\boldsymbol{\kappa}}$ given the eavesdropper's view $\boldsymbol{v}$ is bounded from below by:*

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - 2\left(m + \frac{1}{\ln 2}\right)\left(\theta(r) + 2\sqrt{\theta(r)}\right),$$

*where*

$$\theta(r) = 2^{-\left(1-h\left(\frac{1}{2}-\frac{3}{16}\tau\right)\right)\frac{\tau}{2}r}.$$

*The above bound applies for any value of the security parameter $r$ such that the matrix $K$ specified in the protocol exists.*

The protocol uses previously shared private key for the error reconciliation. A net gain in shared private bits is achieved if $m$ is greater than the number of the secret bits used during error reconciliation. For asymptotic values of $m$, we can take arbitrarily small values for the security parameter and a net gain in private bits is obtained if $m > sh(\epsilon) \simeq \frac{r}{1-\epsilon}h(\epsilon)$. We have seen that privacy amplification is possible if $\frac{m}{r} \leq 1 - h\left(\frac{\epsilon}{1-\epsilon}\right)$. Therefore, a net gain in shared private bits can be obtained for asymptotic values of $m$ if:

$$1 - h\left(\frac{\epsilon}{1-\epsilon}\right) - \frac{1}{1-\epsilon}h(\epsilon) > 0.$$

# 5 Proof of the privacy

## 5.1 Notations

We define the notations used throughout the proof.

**Classical data**

We denote collectively by $C = (\vec{a}, \vec{b}, \vec{\alpha}, \vec{\beta})$ the classical data Alice and Bob generate during the protocol (after the setup). Note that other variables Alice and Bob generate during the protocol can be deterministically derived from $C$. We denote by $P = (\vec{a}, \vec{d}, \vec{e})$ the data that are publicly announced by Alice and Bob during the protocol. Recall that specifying $\vec{a}$ and $\vec{d}$ is equivalent to specifying $\vec{a}$ and $\vec{b}$. For any possible $P$, we denote by $\mathcal{C}_P$ the set of values for the classical data that are compatible with the public announcement of $P$. That is, for a given $P = (\vec{a}, \vec{d}, \vec{e})$,

$$\begin{aligned}\mathcal{C}_P \quad = \quad & \{C' = (\vec{a}', \vec{b}', \vec{\alpha}', \vec{\beta}') \,:\, \vec{a}' = \vec{a}, \\ & \forall i,\, b'_i = a_i \text{ if } d_i = 1,\, b'_i \neq a_i \text{ if } d_i = 0 \\ & \forall i \in E,\, \alpha'_i \neq \beta'_i \text{ and } \forall i \in S \setminus E,\, \alpha'_i = \beta'_i \\ & \text{where } S \text{ and } E \text{ are given by } \vec{d} \text{ and } \vec{e}.\}.\end{aligned}$$

Given a possible $P$ and a value for the private key $\vec{\kappa}$, we define $\mathcal{C}_{P,\vec{\kappa}}$ as the set of values for the classical data that are compatible with the public announcement of $P$ and generation of $\vec{\kappa}$ for the private key. That is, for a given $P = (\vec{a}, \vec{d}, \vec{e})$,

$$\begin{aligned}\mathcal{C}_{P,\vec{\kappa}} \quad = \quad & \{C' = (\vec{a}', \vec{b}', \vec{\alpha}', \vec{\beta}') \,:\, \vec{a}' = \vec{a}, \\ & \forall i,\, b'_i = a_i \text{ if } d_i = 1,\, b'_i \neq a_i \text{ if } d_i = 0 \\ & \forall i \in E,\, \alpha'_i \neq \beta'_i \text{ and } \forall i \in S \setminus E,\, \alpha'_i = \beta'_i \\ & K\alpha'_R = \vec{\kappa} \pmod 2, \\ & \text{ where } S,\, E \text{ and } R \text{ are given by } \vec{d} \text{ and } \vec{e}.\}.\end{aligned}$$

Finally, we denote by $\mathcal{P}$ the set of all possible public announcements for which the validation test is passed. That is,

$$\mathcal{P} = \{P = (\vec{a}, \vec{d}, \vec{e}) \,:\, w(\vec{d}) \geq s \text{ and } e < \epsilon s\}.$$

For any vector $\vec{x}$ and any symbol $A$, $w(\vec{x})$ is the number of non-zero entries, and $w_A(\vec{x})$ is the number of entries with symbol $A$. For any vector $\vec{x} \in \{0,1\}^n$, we denote by $\neg\vec{x}$ the vector whose $i$-th entry is $1 + x_i \pmod 2$ for all $i \in \{1 \ldots n\}$. Finally, we denote by $T$ the subset $S \setminus (E \cup R)$, and by $t$ the size of $T$.

**Bell states**

For each $i \in \{1 \ldots n\}$, we define the Bell basis $\{|\,0\rangle_i, |\,1\rangle_i, |\,2\rangle_i, |\,3\rangle_i\}$ of the $i$-th pair of photons as:

$$\begin{aligned}|\,0\rangle_i \quad &= \quad \frac{|\,0\rangle_{+,i}|\,0\rangle_{+,i} + |\,1\rangle_{+,i}|\,1\rangle_{+,i}}{\sqrt{2}}, \\ |\,1\rangle_i \quad &= \quad \frac{|\,0\rangle_{+,i}|\,0\rangle_{+,i} - |\,1\rangle_{+,i}|\,1\rangle_{+,i}}{\sqrt{2}}, \\ |\,2\rangle_i \quad &= \quad \frac{|\,0\rangle_{+,i}|\,1\rangle_{+,i} + |\,1\rangle_{+,i}|\,0\rangle_{+,i}}{\sqrt{2}}, \\ |\,3\rangle_i \quad &= \quad \frac{|\,0\rangle_{+,i}|\,1\rangle_{+,i} - |\,1\rangle_{+,i}|\,0\rangle_{+,i}}{\sqrt{2}},\end{aligned}$$

where the first and the second state in the product states in the rhs. correspond to Alice's and Bob's $i$-th photon's polarisation state, respectively. Tensor products are implied when we consider state of several photons, that is, $|\,\vec{\alpha}, \vec{\beta}\rangle_{\vec{a},\vec{b}} = \otimes_{i=1}^n |\,\alpha_i\rangle_{a_i,i}|\,\beta_i\rangle_{b_i,i}$ and $|\,\vec{c}\rangle = \otimes_{i=1}^n |\,c_i\rangle_i$. For any subset $X$ of $\{1 \ldots n\}$, $|\,\alpha_X, \beta_X\rangle_{a_X,b_X} = \otimes_{i\in X} |\,\alpha_i\rangle_{a_i,i}|\,\beta_i\rangle_{b_i,i}$.

Given a basis $a \in \{+, \times\}$, we define $X_a$ as the set of indexes of Bell states that are compatible with Alice and Bob measuring in the same basis $a$ and sharing the same bit value. Likewise, we define $Y_a$ as the set of indexes of Bell states that are compatible with Alice and Bob measuring in basis $a$ and not sharing the same bit value. That is, $X_+ = \{0,1\}$, $X_\times = \{0,2\}$, $Y_+ = \{2,3\}$ and $Y_\times = \{1,3\}$. Given the choice of bases $\vec{a}$ and a set $A \subset \{1 \ldots n\}$, we define $X_{a_A}$ as $\{c_A \in \{0,1,2,3\}^A \,:\, \forall i \in A, c_i \in X_{a_i}\}$ and $Y_{a_A}$ as $\{c_A \in \{0,1,2,3\}^A \,:\, \forall i \in A, c_i \in Y_{a_i}\}$. Given a reconciled set $R$

and the choice of bases $a_R$ on $R$, for any $c_R \in X_{a_R}$, we will denote by $\vec{\gamma}$ the unique $\vec{\gamma} \in \{0,1\}^r$ such that for each $i \in \{1,\ldots,r\}$, $c_i = (1+w_\times a_i)\gamma_i$, i.e. $c_i = \gamma_i$ if $a_i = +$, and $c_i = 2\gamma_i$ if $a_i = \times$. For any vectors $\vec{x}$, $\vec{y} \in \{0,1\}^r$, we define $\vec{x}\cdot\vec{y}$ as $\vec{x}\cdot\vec{y} \stackrel{Def}{=} \sum_{i=1}^r x_i y_i$. Given $R$ and $a_R$, for any $c_R \in X_{a_R}$, we have the identity ${}_{a_R}\langle \alpha_R, \alpha_R | c_R \rangle = \frac{(-1)^{\alpha_R\cdot\vec{\gamma}}}{\sqrt{2^r}}$.

## 5.2 Model of measurements

A mathematical model of measurements on the quantum state generated by the source is given. The source can be under complete control of Eve, as long as it sends $n$ single photons to both Alice and Bob. In such a scenario, Eve may entangle a probe of any dimension to the photons she sends to Alice and Bob which are in any state Eve wants. We write the state of these $n$ couples of photons and the probe in the Bell basis as follows:

$$\rho = \sum_{\vec{c},\vec{c}'} |\, E_{\vec{c}}\rangle\langle E_{\vec{c}'}\,| \otimes |\,\vec{c}\rangle\langle\vec{c}'\,|,$$

where the states $|\, E_{\vec{c}}\rangle$ are states of Eve's probe that are possibly nor orthogonal nor normalised. The positive operator giving the probability that Alice and Bob get $C = (\vec{a},\vec{b},\vec{\alpha},\vec{\beta})$ as their classical data is simply:

$$F_C = \mathrm{P}_{\vec{a}}(\vec{a})\mathrm{P}_{\vec{b}}(\vec{b})|\,\vec{\alpha},\vec{\beta}\rangle_{\vec{a},\vec{b}\ \vec{a},\vec{b}}\langle\vec{\alpha},\vec{\beta}\,|,$$

where $\mathrm{P}_{\vec{a}}(\vec{a}) = 1/2^n$ and $\mathrm{P}_{\vec{b}}(\vec{b}) = 1/2^n$ for any choice of $\vec{a}$ and $\vec{b}$. Note that $\mathrm{P}_{\vec{a}}(\vec{a})\mathrm{P}_{\vec{b}}(\vec{b}) = \mathrm{P}_{\vec{a}}(\vec{a})\mathrm{P}_{\vec{d}}(\vec{d})$ where $\mathrm{P}_{\vec{d}} = 1/2^n$.

The positive operator giving the probability that Alice and Bob publicly announce $P = (\vec{a},\vec{d},\vec{e})$ while they get the private key $\vec{\kappa}$ is the sum of the operators $F_{C'}$ for $C'$ running over $\mathcal{C}_{P,\vec{\kappa}}$:

$$\begin{aligned}
F_{P,\vec{\kappa}} &= \sum_{C'\in\mathcal{C}_{P,\vec{\kappa}}} \mathrm{P}_{\vec{a}}(\vec{a}')\mathrm{P}_{\vec{d}}(\vec{d}')|\,\vec{\alpha}',\vec{\beta}'\rangle_{\vec{a}',\vec{b}'\ \vec{a}',\vec{b}'}\langle\vec{\alpha}',\vec{\beta}'\,| \\
&= \mathrm{P}_{\vec{a}}(\vec{a})\mathrm{P}_{\vec{d}}(\vec{d})\mathbf{1}_{\overline{S}} \otimes \sum_{\alpha_E\in\{0,1\}^e} |\,\alpha_E,\neg\alpha_E\rangle_{a_E,a_E\ a_E,a_E}\langle\alpha_E,\neg\alpha_E\,| \\
&\quad \otimes \sum_{\alpha_T\in\{0,1\}^t} |\,\alpha_T,\alpha_T\rangle_{a_T,a_T\ a_T,a_T}\langle\alpha_T,\alpha_T\,| \\
&\quad \otimes \sum_{\substack{\alpha_R\in\{0,1\}^r:\\ K\alpha_R=\vec{\kappa}}} |\,\alpha_R,\alpha_R\rangle_{a_R,a_R\ a_R,a_R}\langle\alpha_R,\alpha_R\,|
\end{aligned}$$

where $\mathbf{1}_{\overline{S}}$ is the identity operator acting on the Hilbert space describing photons not in $S$. Note that $\vec{b}(S) = \vec{a}(S)$.

Similarly, the positive operator giving the marginal probability that Alice and Bob publicly announce $P = (\vec{a},\vec{d},\vec{e})$ is the sum of the operators $F_{C'}$ for $C'$

running over $\mathcal{C}_P$:

$$\begin{aligned} F_P &= \sum_{C' \in \mathcal{C}_P} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a}')\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}')\,|\,\vec{\alpha}', \vec{\beta}'\rangle_{\vec{a}',\vec{b}'\ \vec{a}',\vec{b}'}\langle\vec{\alpha}', \vec{\beta}'\,| \\ &= \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d})\mathbf{1}_{\overline{S}} \otimes \sum_{\alpha_E \in \{0,1\}^e} |\,\alpha_E, \neg\alpha_E\rangle_{a_E,a_E\ a_E,a_E}\langle\alpha_E, \neg\alpha_E\,| \\ &\quad \otimes \sum_{\alpha_T \in \{0,1\}^t} |\,\alpha_T, \alpha_T\rangle_{a_T,a_T\ a_T,a_T}\langle\alpha_T, \alpha_T\,| \\ &\quad \otimes \sum_{\alpha_R \in \{0,1\}^r} |\,\alpha_R, \alpha_R\rangle_{a_R,a_R\ a_R,a_R}\langle\alpha_R, \alpha_R\,|. \end{aligned}$$

Eve may perform a general measurement on her probe. This general measurement can take place after Alice and Bob's public announcements and therefore can be conditioned on $\boldsymbol{P}$. We will denote by $\mathcal{V}_P$ the set of views $v$ that are compatible with the public announcement $P$. The positive operator giving the probability that Eve gets the view $v$ given that Alice and Bob announced $P$ will be denoted by $G_{v|P}$. We will assume without loss of generality that the operators $G_{v|P}$ are of rank one, i.e. $G_{v|P} = |\,\chi_{v|P}\rangle\langle\chi_{v|P}\,|$ where the vectors $|\,\chi_{v|P}\rangle$ are possibly not orthogonal nor normalised, but obey the relation $\sum_{v\in\mathcal{V}_P} G_{v|P} = \mathbf{1}$.

## 5.3 The rôle of the validation test

Here we show that it is very unlikely that the validation test is passed when the state of the photons emitted by the source is very different from the ideal state specified by the protocol. The underlying principle has been advanced in [14, 17, 18]. More precisely, given a possible reconciled set $R$, let $\Pi_R$ be the orthogonal projection operator defined as:

$$\begin{aligned} \Pi_R &= \sum_{\substack{\vec{c}\in\{0,1,2,3\}^n : \\ w(c_R)\geq d_K/2}} |\,\vec{c}\rangle\langle\vec{c}\,| \\ &= \mathbf{1}_{\overline{R}} \otimes \sum_{\substack{c_R\in\{0,1,2,3\}^r : \\ w(c_R)\geq d_K/2}} |\,c_R\rangle\langle c_R\,|. \end{aligned}$$

The operator $\Pi_R$ projects onto Bell states for pairs of photons in $R$ with weight greater than $d_K/2 = \left(\frac{\epsilon}{1-\epsilon} + \frac{\tau}{2}\right) r$. The following property is then proved.

**Property 2** *The eigenvalues of the semi-definite positive Hermitian operator*

$$\sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R,$$

*where $R$ is specified by $P$ in the sum, are bounded from above by*

$$\theta(r) = 2^{-\left(1-h\left(\frac{1}{2}-\frac{3}{16}\tau\right)\right)\frac{\tau}{2}r}.$$

**Proof** The above operator can be written as:

$$\sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R = \sum_{\substack{\vec{d}\in\{0,1\}^n:\\ w(\vec{d})\geq s}} \sum_{\substack{\vec{e}\in\{0,1\}^s:\\ w(\vec{e})<\epsilon s}} \Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R.$$

Now for given $\vec{d}$ and $\vec{e}$,

$$\sum_{\vec{a}} F_P = \mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \mathbf{1}_{\overline{S}} \otimes_{i\in E} Y_i \otimes_{j\in T} X_j \otimes_{k\in R} X_k,$$

where

$$\begin{aligned} X_i &= |\,0\rangle\langle 0\,| + \frac{1}{2}|\,1\rangle\langle 1\,| + \frac{1}{2}|\,2\rangle\langle 2\,|, \\ Y_i &= |\,3\rangle\langle 3\,| + \frac{1}{2}|\,1\rangle\langle 1\,| + \frac{1}{2}|\,2\rangle\langle 2\,| \end{aligned}$$

are operators acting on $i$-th photon pair's Hilbert space. The last equalities are derived directly from the definition of the Bell states. As a consequence, we have,

$$\Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R = \mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \mathbf{1}_{\overline{S}} \otimes_{i\in E} Y_i \otimes_{j\in T} X_j \otimes \Big( \sum_{\substack{c_R\in\{0,1,2\}:\\ w(c_R)\geq d_K/2}} \frac{|\,c_R\rangle\langle c_R\,|}{2^{w_1(c_R)+w_2(c_R)}} \Big).$$

Now, given $\vec{d}\in\{0,1\}^n$, the operator:

$$\sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R$$

is diagonal in the Bell basis $|\,c\rangle$. Given a vector $\vec{c}\in\{0,1,2,3\}^n$ and an error vector $\vec{e}\in\{0,1\}^s$, a necessary condition for the scalar:

$$\langle c\,|\Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R|\,c\rangle$$

to be non zero is that, for all $i\in S$,

- $e_i = 0$ if $c_i = 0$,
- $e_i = 1$ if $c_i = 3$, and
- $w_1(c_S) + w_2(c_S) \geq e - w_3(c_S) + d_K/2$ (otherwise $w(c_R)$ is smaller than $d_K/2$).

Let $k = e - w_3(c_S)$. Then there are $\binom{w_1(c_S)+w_2(c_S)}{k}$ such vectors $\vec{e}$ of weight $e$, if $0 \leq k < \epsilon s - w_3(c_S)$ and $k \leq w_1(c_S) + w_2(c_S) - d_K/2$. Therefore,

$$\begin{aligned}
&\langle c \,| \sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left( \sum_{\vec{a}} F_P \right) \Pi_R |\, c\rangle \\
&\quad \leq \frac{\mathrm{P}_{\vec{d}}(\vec{d})}{2^{w_1(c_S)+w_2(c_S)}} \sum_{\substack{0\leq k<\epsilon s - w_3(c_S), \text{ and} \\ k\leq w_1(c_S)+w_2(c_S)-\frac{d_K}{2}}} \binom{w_1(c_S)+w_2(c_S)}{k}.
\end{aligned}$$

Now, $d_K$ is either greater or smaller than $(w_1(c_S) + w_2(c_S))\left(1 + \frac{\tau}{2}(1-\epsilon)\right)$.

- If $d_K > (w_1(c_S) + w_2(c_S))\left(1 + \frac{\tau}{2}(1-\epsilon)\right)$, then

$$w_1(c_S) + w_2(c_S) - \frac{d_K}{2} < \frac{1}{2}\left(1 - \frac{\tau}{2}(1-\epsilon)\right)(w_1(c_S) + w_2(c_S)) \text{ and,}$$

- if $d_K \leq (w_1(c_S) + w_2(c_S))\left(1 + \frac{\tau}{2}(1-\epsilon)\right)$, then

$$\begin{aligned}
\epsilon s - w_3(c_S) &\leq \frac{\epsilon r}{1-\epsilon} \\
&= \frac{d_K}{2} - \frac{\tau}{2} r \\
&\leq \frac{1}{2}\left(1 - \frac{\tau}{2}(1-\epsilon)\right)(w_1(c_S) + w_2(c_S)),
\end{aligned}$$

where we have used $r \geq s(1-\epsilon)$ and $s \geq w_1(c_S) + w_2(c_S)$.

We thus derived that:

$$\begin{aligned}
&\langle c \,| \sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left( \sum_{\vec{a}} F_P \right) \Pi_R |\, c\rangle \\
&\leq \frac{\mathrm{P}_{\vec{d}}(\vec{d})}{2^{w_1(c_S)+w_2(c_S)}} \sum_{0\leq k<\frac{1}{2}\left(1-\frac{\tau}{2}(1-\epsilon)\right)(w_1(c_S)+w_2(c_S))} \binom{w_1(c_S)+w_2(c_S)}{k} \\
&\leq \mathrm{P}_{\vec{d}}(\vec{d}) 2^{-\left(1-h\left(\frac{1}{2}\left(1-\frac{\tau}{2}(1-\epsilon)\right)\right)\right)(w_1(c_S)+w_2(c_S))} \\
&\leq \mathrm{P}_{\vec{d}}(\vec{d}) 2^{-\left(1-h\left(\frac{1}{2}-\frac{3}{16}\tau\right)\right)\frac{\tau}{2}r} \\
&= \mathrm{P}_{\vec{d}}(\vec{d})\theta(r)
\end{aligned}$$

where we have used the binomial inequality stating that $\sum_{0\leq k<pn}\binom{n}{k} \leq 2^{nh(p)}$ for any positive integer $n$ and $0 \leq p < 1/2$. In the last inequality we have used the inequalities $\epsilon < 1/4$ and $w_1(c_S) + w_2(c_S) \geq d_K/2$ when the above scalar is non zero.

Remarking that the operator $\sum_{\vec{a},\vec{e}\,:\ e<\epsilon s} \Pi_R F_P \Pi_R$ is diagonal in the Bell basis for all $\vec{d}$ and $\sum_{\vec{d}\,:\, w(\vec{d})\geq s} \mathrm{P}_{\vec{d}}(\vec{d}) \leq 1$, this concludes the proof. □

We recall that $\rho = \sum_{\vec{c},\vec{c}'} |\, E_{\vec{c}}\rangle\langle E_{\vec{c}'}\,| \otimes |\,\vec{c}\rangle\langle\vec{c}'\,|$ is the density operator describing Alice and Bob's photons and Eve's probe. The above property implies that:

$$\mathrm{Tr}\Big(\mathbf{1}_{\mathrm{Eve}} \otimes \sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R \rho\Big) \leq \theta(r)$$

where $\mathbf{1}_{\mathrm{Eve}}$ is the identity operator acting on the Hilbert space of the probe. That is,

$$\sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\substack{c_R\in X_{a_R}:\\ w(c_R)\geq d_K/2}} \langle E_{\vec{c}}\,|\,E_{\vec{c}}\rangle \leq \theta(r).$$

## 5.4 Quasi-independence of the key and the view

In this section we compute the joint probability distribution of the key and the view. We prove that this distribution is very close to a product of an uniform distribution for the key and the marginal probability distribution of the view.

**Property 3** *For any given eavesdropping strategy chosen by Eve and returning a view $\boldsymbol{v}$, the probability distribution of the key $\vec{\boldsymbol{\kappa}}$ and the view $\boldsymbol{v}$ obeys the following inequality:*

$$\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m} \left|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\right| \leq 2\left(\theta(r)+2\sqrt{\theta(r)}\right)$$

*where $m$ is the length of the private key and $r$ is the size of the reconciled set.*

**Proof** For any $\vec{\kappa}\in\{0,1\}^m$, $P$ and $v\in\mathcal{V}_P$, we have:

$$\begin{aligned}
&\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\\
&\quad= \mathrm{Tr}(G_{v|P}\otimes F_{P,\vec{\kappa}}\,\rho) - \frac{1}{2^m}\mathrm{Tr}(G_{v|P}\otimes F_P\,\rho)\\
&\quad= \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{\vec{c},\vec{c}':\\ c_E,c'_E\in Y_{a_E},\\ c_T,c'_T\in X_{a_T},\\ c_R,c'_R\in X_{a_R}}} \langle E_{\vec{c}'}\,|G_{v|P}|\,E_{\vec{c}}\rangle \delta_{c_{\overline{R}},c'_{\overline{R}}} d_{\vec{\kappa}}(\vec{\gamma},\vec{\gamma}'),
\end{aligned}$$

where

$$d_{\vec{\kappa}}(\vec{\gamma},\vec{\gamma}') = \sum_{\substack{\alpha_R\in\{0,1\}^r:\\ K\alpha_R=\vec{\kappa} \pmod 2}} \frac{(-1)^{\alpha_R\cdot(\vec{\gamma}+\vec{\gamma}')}}{2^r} - \frac{1}{2^m}\delta_{\vec{\gamma},\vec{\gamma}'}.$$

where we have used the identity ${}_{a_R,a_R}\langle\alpha_R,\alpha_R\,|c_R\rangle = \frac{(-1)^{\alpha_R\cdot\vec{\gamma}}}{\sqrt{2^r}}$ for any $c_R\in X_{a_R}$. We denote by:

- $\mathcal{G}$ the set of all linear combinations over $\{0,1\}$ of rows of $K$. It is a vector space of dimension $m$.
- $\mathcal{S}$ a subspace of $\{0,1\}^r$ that is supplement to the subspace $\mathcal{G}$, that is $\mathcal{G}\oplus\mathcal{S}=\{0,1\}^r$. The dimension of $\mathcal{S}$ is $r-m$.

- $\mathcal{K}$ the set of all vectors $\vec{x} \in \{0,1\}^r$ such that $K\vec{x} = \vec{0} \pmod 2$. The set $\mathcal{K}$ is a vector space of dimension $r-m$, since the rows of $K$ are linearly independent. We will denote by $\{\vec{u}_1, \ldots, \vec{u}_{r-m}\}$ a basis of $\mathcal{K}$.

Given a subspace $F$ of $\{0,1\}^r$, we denote by $F^\perp$ the set of all vectors $\vec{x} \in \{0,1\}^r$ such that for all $\vec{y} \in F$, $\vec{x} \cdot \vec{y} = 0 \pmod 2$. Remark that $\mathcal{K}^\perp = \mathcal{G}$. Since the rows of $K$ are linearly independent, for any $\vec{\kappa} \in \{0,1\}^m$, there exists a vector $\vec{\theta}_{\vec{\kappa}} \in \{0,1\}^r$ such that $K\vec{\theta}_{\vec{\kappa}} = \vec{\kappa} \pmod 2$. It follows that $K\alpha_{_R} = \vec{\kappa} \pmod 2$ if and only if $\alpha_{_R} \in \vec{\theta}_{\vec{\kappa}} + \mathcal{K}$. Thus following the techniques used in [13],

$$\begin{aligned}
\sum_{\substack{\alpha_{_R} \in \{0,1\}^r : \\ K\alpha_{_R} = \vec{\kappa} \pmod 2}} (-1)^{\alpha_{_R} \cdot (\vec{\gamma} + \vec{\gamma}')} &= \sum_{\alpha_{_R} \in \vec{\theta}_{\vec{\kappa}} + \mathcal{K}} (-1)^{\alpha_{_R} \cdot (\vec{\gamma} + \vec{\gamma}')} \\
&= (-1)^{\vec{\theta}_{\vec{\kappa}} \cdot (\vec{\gamma} + \vec{\gamma}')} \prod_{i=1}^{r-m} \left[1 + (-1)^{\vec{u}_i \cdot (\vec{\gamma} + \vec{\gamma}')}\right] \\
&= \begin{cases} (-1)^{\vec{\theta}_{\vec{\kappa}} \cdot (\vec{\gamma} + \vec{\gamma}')} 2^{r-m} & \text{if } \vec{\gamma} + \vec{\gamma}' \in \mathcal{K}^\perp = \mathcal{G}, \\ 0 & \text{if } \vec{\gamma} + \vec{\gamma}' \notin \mathcal{G}. \end{cases}
\end{aligned}$$

One obtains therefore that:

$$\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v) = \frac{1}{2^m}\mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}} : \\ c_E \in Y_{a_E}, \\ c_T \in X_{a_T}}} (U_{v\vec{\kappa}c_{\overline{R}}} + V_{v\vec{\kappa}c_{\overline{R}}})^\dagger \Delta (U_{v\vec{\kappa}c_{\overline{R}}} + V_{v\vec{\kappa}c_{\overline{R}}}),$$

where $U_{v\vec{\kappa}c_{\overline{R}}}$ and $V_{v\vec{\kappa}c_{\overline{R}}}$ are complex vectors of dimension $2^r$ and $\Delta$ is a $2^r \times 2^r$ complex matrix, whose entries are indexed by $\vec{\gamma} \in \{0,1\}^r$. The $\vec{\gamma}$-th entry of $U_{v\vec{\kappa}c_{\overline{R}}}$ and $V_{v\vec{\kappa}c_{\overline{R}}}$ are:

$$\begin{aligned}
\left(U_{v\vec{\kappa}c_{\overline{R}}}\right)_{\vec{\gamma}} &= \begin{cases} (-1)^{\vec{\theta}_{\vec{\kappa}} \cdot \vec{\gamma}} \langle \chi_{v|P} \, | E_{\vec{c}} \rangle & \text{if } w(\vec{\gamma}) < d_K/2, \\ 0 & \text{if } w(\vec{\gamma}) \geq d_K/2. \end{cases} \\
\left(V_{v\vec{\kappa}c_{\overline{R}}}\right)_{\vec{\gamma}} &= \begin{cases} 0 & \text{if } w(\vec{\gamma}) < d_K/2, \\ (-1)^{\vec{\theta}_{\vec{\kappa}} \cdot \vec{\gamma}} \langle \chi_{v|P} \, | E_{\vec{c}} \rangle & \text{if } w(\vec{\gamma}) \geq d_K/2, \end{cases}
\end{aligned}$$

where $\vec{c}$ is given by $c_{\overline{R}}$, $a_{_R}$ and $\vec{\gamma}$. The $(\vec{\gamma}, \vec{\gamma}')$-th entry of $\Delta$ is:

$$\left(\Delta\right)_{\vec{\gamma},\vec{\gamma}'} = \begin{cases} 1 & \text{if } \vec{\gamma} + \vec{\gamma}' \in \mathcal{G} \setminus \{0\}, \\ 0 & \text{if } \vec{\gamma} + \vec{\gamma}' \notin \mathcal{G} \setminus \{0\}. \end{cases}$$

This implies $U^\dagger_{v\vec{\kappa}c_{\overline{R}}} \Delta U_{v\vec{\kappa}c_{\overline{R}}} = 0$, since $w(\vec{\gamma}) < d_K/2$ and $w(\vec{\gamma}') < d_K/2$ imply that $w(\vec{\gamma} + \vec{\gamma}') < d_K$, that is, $\vec{\gamma} + \vec{\gamma}' \notin \mathcal{G} \setminus \{\vec{0}\}$.

The matrix $\Delta$ is Hermitian, of eigenvalues $2^m - 1$ and $-1$. There are $2^{r-m}$ eigenvectors $\vec{v}_{\vec{x}}$ ($\vec{x} \in \mathcal{S}$) associated with the eigenvalue $2^m - 1$. The $\vec{\gamma}$-th entry of $\vec{v}_{\vec{x}}$ is:

$$\left(\vec{v}_{\vec{x}}\right)_{\vec{\gamma}} = \begin{cases} 1 & \text{if } \vec{\gamma} + \vec{x} \in \mathcal{G} \\ 0 & \text{if } \vec{\gamma} + \vec{x} \notin \mathcal{G}. \end{cases}$$

There are $2^{r-m}\,(2^m-1)$ eigenvectors $\vec{w}_{\vec{x},\vec{\sigma}}$ ($\vec{x}\in\mathcal{S}$, $\vec{\sigma}\in\{0,1\}^m\setminus\{\vec{0}\}$) associated with the eigenvalue $-1$. The $\vec{\gamma}$-th entry of $\vec{w}_{\vec{x},\vec{\sigma}}$ is:

$$\left(\vec{w}_{\vec{x},\vec{\sigma}}\right)_{\vec{\gamma}} = \begin{cases} (-1)^{\vec{\omega}_{\vec{\gamma}+\vec{x}}\cdot\vec{\sigma}} & \text{if } \vec{\gamma}+\vec{x}\in\mathcal{G} \\ 0 & \text{if } \vec{\gamma}+\vec{x}\notin\mathcal{G}. \end{cases}$$

where for any $\vec{y}\in\mathcal{G}$, $\vec{\omega}_{\vec{y}}$ is the unique vector in $\{0,1\}^m$ such that $K^T\vec{\omega}_{\vec{y}}=\vec{y}\pmod 2$. Note that for any $\vec{\gamma}\in\{0,1\}^r$, there is an unique $(\vec{x},\vec{y})\in\mathcal{S}\times\mathcal{G}$ such that $\vec{\gamma}=\vec{x}+\vec{y}$, and that:

$$\mathbf{1}_{\vec{\gamma}} = \frac{1}{2^m}\left(\vec{v}_x + \sum_{\vec{\sigma}\in\{0,1\}^m\setminus\{\vec{0}\}} (-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{\sigma}}\vec{w}_{\vec{x},\vec{\sigma}}\right),$$

where $\mathbf{1}_{\vec{\gamma}}$ is the canonical vector with entry 1 at position $\vec{\gamma}$ and 0 everywhere else. We can express the vectors $U_{v\vec{\kappa}c_{\overline{R}}}$ and $V_{v\vec{\kappa}c_{\overline{R}}}$ as linear combinations of these eigenvectors:

$$\begin{aligned} U_{v\vec{\kappa}c_{\overline{R}}} &= \sum_{\vec{x}\in\mathcal{S}}(-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{x}}\phi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}\vec{v}_{\vec{x}} + \sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\sigma}\neq\vec{0}}(-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{x}}\phi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}\vec{w}_{\vec{x},\vec{\sigma}}, \\ V_{v\vec{\kappa}c_{\overline{R}}} &= \sum_{\vec{x}\in\mathcal{S}}(-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{x}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}\vec{v}_{\vec{x}} + \sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\sigma}\neq\vec{0}}(-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{x}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}\vec{w}_{\vec{x},\vec{\sigma}}, \end{aligned}$$

where for any $\vec{z}\in\{0,1\}^m$,

$$\begin{aligned} \phi_{v,c_{\overline{R}},\vec{x},\vec{z}} &= \sum_{\substack{\vec{y}\in\mathcal{G}:\\ w(\vec{x}+\vec{y})<d_K/2}} \frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle, \\ \psi_{v,c_{\overline{R}},\vec{x},\vec{z}} &= \sum_{\substack{\vec{y}\in\mathcal{G}:\\ w(\vec{x}+\vec{y})\geq d_K/2}} \frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle. \end{aligned}$$

In deriving the above formulae, we used the identity $\vec{\theta}_{\vec{\kappa}}\cdot\vec{y}=\vec{\omega}_{\vec{y}}\cdot\vec{\kappa}\pmod 2$ for any $\vec{y}\in\mathcal{G}$ and $\vec{\kappa}\in\{0,1\}^m$. It follows that:

$$\begin{aligned} V^\dagger_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}} &= \sum_{\vec{x}\in\mathcal{S}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2(2^m-1)\|\vec{v}_{\vec{x}}\|^2 - \sum_{\substack{\vec{x}\in\mathcal{S}\\ \vec{\sigma}\neq\vec{0}}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}|^2\|\vec{w}_{\vec{x},\vec{\sigma}}\|^2 \\ &= 2^m\Big[(2^m-1)\sum_{\vec{x}\in\mathcal{S}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2 - \sum_{\substack{\vec{x}\in\mathcal{S}\\ \vec{\sigma}\neq\vec{0}}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}|^2\Big], \end{aligned}$$

thus,

$$\begin{aligned} &\sum_{\vec{\kappa}\in\{0,1\}^m}\left|V^\dagger_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}}\right| \\ &\leq 2^m\sum_{\vec{x}\in\mathcal{S}}\Big[(2^m-1)\sum_{\vec{\kappa}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2 + \sum_{\vec{\sigma}\neq\vec{0},\vec{\kappa}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}|^2\Big] \\ &= 2^{m+1}(2^m-1)\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2. \end{aligned}$$

Similarly, we have,

$$\sum_{\vec{\kappa}\in\{0,1\}^m}\left|U^{\dagger}_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}}\right| \leq 2^{m+1}(2^m-1)\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}|\phi^*_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|.$$

Now,

$$\begin{aligned}
&\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\right| \\
&\quad\leq \sum_{P\in\mathcal{P}}\frac{1}{2^m}\mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d})\sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m}\left[|V^{\dagger}_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}}|+2|U^{\dagger}_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}}|\right] \\
&\quad\leq 2(2^m-1)\sum_{P\in\mathcal{P}}\mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d})\sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\left[|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2+2|\phi^*_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|\right] \\
&\quad\leq 2(2^m-1)(\eta+2\sqrt{\eta}\sqrt{\xi}),
\end{aligned}$$

where we used the Schwartz inequality, and where

$$\begin{aligned}
\eta &= \sum_{P\in\mathcal{P}}\sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d})|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2, \\
\xi &= \sum_{P\in\mathcal{P}}\sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d})|\phi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2.
\end{aligned}$$

We derive an upper-bound on $\eta$ and $\xi$. We have:

$$\begin{aligned}
\eta &= \sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}} \sum_{\substack{\vec{y},\vec{y}'\in\mathcal{G}\\ w(\vec{x}+\vec{y})\geq d_K/2\\ w(\vec{x}+\vec{y}')\geq d_K/2}} \sum_{\vec{\kappa}} \frac{(-1)^{\vec{\omega}_{\vec{y}+\vec{y}'}\cdot\vec{\kappa}}}{2^{2m}} \langle E_{\vec{c}'} \,|\, \chi_{v|P}\rangle\langle\chi_{v|P} \,|\, E_{\vec{c}}\rangle \\
&= \frac{1}{2^m}\sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\vec{x}\in\mathcal{S}} \sum_{\substack{\vec{y}\in\mathcal{G}\\ w(\vec{x}+\vec{y})\geq d_K/2}} \sum_{v\in\mathcal{V}_P} \langle E_{\vec{c}} \,|\, \chi_{v|P}\rangle\langle\chi_{v|P} \,|\, E_{\vec{c}}\rangle \\
&= \frac{1}{2^m}\sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\substack{\vec{x}\in\mathcal{S},\,\vec{y}\in\mathcal{G}\\ w(\vec{x}+\vec{y})\geq d_K/2}} \langle E_{\vec{c}} \,|\, E_{\vec{c}}\rangle \\
&= \frac{1}{2^m}\sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\substack{c_R\in X_{a_R}:\\ w(c_R)\geq d_K/2}} \langle E_{\vec{c}} \,|\, E_{\vec{c}}\rangle \\
&\leq \frac{1}{2^m}\theta(r),
\end{aligned}$$

using the result of the previous section. Similarly,

$$\begin{aligned}
\xi &= \frac{1}{2^m}\sum_{P\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{a}}}(\vec{a})\mathrm{P}_{\vec{\boldsymbol{d}}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\substack{c_R\in X_{a_R}:\\ w(c_R)<d_K/2}} \langle E_{\vec{c}} \,|\, E_{\vec{c}}\rangle \\
&\leq \frac{1}{2^m}.
\end{aligned}$$

Consequently,

$$\begin{aligned}
&\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m} \left|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\right| \\
&\qquad \leq 2\left(\theta(r) + 2\sqrt{\theta(r)}\right)
\end{aligned}$$

which concludes our proof. □

## 5.5 Bound on the conditional entropy

We conclude the proof of privacy by using the following property from classical information theory.

**Property 4** *Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two discrete random variables taking values in the sets $\mathcal{X}$ and $\mathcal{Y}$ respectively. Let $\mu$ be a nonnegative real number. If the following*

*inequality is satisfied:*

$$\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \left| \mathrm{P}_{\boldsymbol{xy}}(x,y) - \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y) \right| \leq \mu,$$

*then the conditional entropy of* $\boldsymbol{x}$ *given* $\boldsymbol{y}$ *is lower-bounded by:*

$$H(\boldsymbol{x}|\boldsymbol{y}) \geq (1-\mu)\log_2|\mathcal{X}| - \frac{1}{\ln 2}\mu.$$

**Proof** The hypothesis implies that there exist a set of real numbers $\eta_{x,y}$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that:

$$\mathrm{P}_{\boldsymbol{xy}}(x,y) = \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)(1+\eta_{x,y}),$$

($\eta_{x,y}$ is assigned the value zero if $\mathrm{P}_{\boldsymbol{y}}(y) = 0$) obeying the inequality:

$$\sum_{x\in\mathcal{X},y\in\mathcal{Y}} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)|\eta_{x,y}| \leq \mu.$$

Note that for all $x$ and $y$, we have $-1 \leq \eta_{x,y} \leq |\mathcal{X}| - 1$. Now,

$$\begin{aligned}
H(\boldsymbol{x}|\boldsymbol{y}) &= -\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}\,:\,\mathrm{P}_{\boldsymbol{xy}}(x,y)>0} \mathrm{P}_{\boldsymbol{xy}}(x,y)\log_2 \mathrm{P}_{\boldsymbol{x}\,|\,\boldsymbol{y}=y}(x) \\
&= \log_2|\mathcal{X}| - \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}\,:\,\eta_{x,y}>-1} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)\underbrace{\log_2(1+\eta_{x,y})}_{\leq \frac{|\eta_{x,y}|}{\ln 2}} \\
&\quad - \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}\,:\,\eta_{x,y}>-1} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)\eta_{x,y}\log_2 \underbrace{(1+\eta_{x,y})}_{\leq|\mathcal{X}|} \\
&\geq \log_2|\mathcal{X}| - \frac{\mu}{\ln 2} - \mu\log_2|\mathcal{X}|,
\end{aligned}$$

which concludes the proof. □

The probability distribution of the private key and the view obeys the following inequality:

$$\begin{aligned}
&\sum_{\substack{\vec{\kappa}\in\{0,1\}^m,\\ v\in\mathcal{V}}} \left| \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v) \right| \\
&\leq \sum_{P\in\mathcal{P}} \sum_{\substack{v\in\mathcal{V}_P,\\ \vec{\kappa}\in\{0,1\}^m}} \left| \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{\mathrm{P}_{\boldsymbol{v}}(v)}{2^m} \right| + \sum_{P\notin\mathcal{P}} \sum_{\substack{v\in\mathcal{V}_P,\\ \vec{\kappa}\in\{0,1\}^m}} \left| \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{\mathrm{P}_{\boldsymbol{v}}(v)}{2^m} \right| \\
&\leq 2(\theta(r) + 2\sqrt{\theta(r)}) + 0.
\end{aligned}$$

where we have used the fact that the key is randomly chosen by Alice with uniform probability distribution if the validation test is not passed. Applying the above property for the random variables $\vec{\boldsymbol{\kappa}}$ and $\boldsymbol{v}$, we obtain:

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - 2\left(m + \frac{1}{\ln 2}\right)\left(\theta(r) + 2\sqrt{\theta(r)}\right),$$

which concludes the proof of privacy. □

**Acknowledgement** The author gratefully acknowledges support provided by the European TMR Network ERP-4061PL95-1412, and thanks Hans Briegel, Artur Ekert, Nicolas Gisin, Patrick Hayden, Norbert Lütkenhaus, Dominic Mayers, Michele Mosca, Luke Rallan, Peter Shor and Vlatko Vedral for interesting discussions and helpful comments.

# References

[1] C. H. Bennett and G. Brassard. Quantum cryptography, public key distribution and coin tossing. In *Proceedings of International Conference on Computer Systems and Signal Processing*, page 175, 1984.

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121, 1992.

[3] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661, 1991.

[4] B. Huttner and A. Ekert. Tolerable noise in quantum cryptosystems. *J. Mod. Opt.*, 41:2455, 1994.

[5] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy. *Phys. Rev. A*, 56:1163, 1997.

[6] B. Slutsky, R. Rao, P.-C Sun, and Y. Fainman. Security of quantum cryptography against individual attacks. *Phys. Rev. A*, 57:2383, 1998.

[7] N. Lütkenhaus. Security against eavesdropping in quantum cryptography. *Phys. Rev. A*, 54:97, 1996.

[8] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996.

[9] J. I. Cirac and N. Gisin. Coherent eavesdropping strategies for the 4 state quantum cryptography protocol. *Phys. Lett. A*, 229:1, 1997.

[10] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59:3301, 1999.

[11] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

[12] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances Cryptology — Proceedings of Crypto '96*, page 343, 1996.

[13] D. Mayers. Unconditional security in quantum cryptography. quant-ph/9802025, 1998.

[14] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050, 1999.

[15] H.-K. Lo. A simple proof of the unconditional security of quantum key distribution. quant-ph/9904091, 1999.

[16] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution. quant-ph/9912053, 1999.

[17] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. quant-ph/0003004, 2000.

[18] M. Ben-Or. Manuscript in preparation.

[19] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557, 1992.

[20] H. Aschauer and H. Briegel. Secure quantum communication over arbitrary distances. quant-ph/0008051, 2000.

[21] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science*, 1998.

[22] D. Mayers. Manuscript in preparation.

[23] H. Inamori, N. Lütkenhaus, and D. Mayers. Security of practical quantum key distribution. Manuscript in preparation.

[24] C. E. Shannon. *Bell Syst. Tech. J*, 28:656, 1949.

[25] D. Welsh. *Codes and cryptography*. Clarendon Press, Oxford, 1988.

[26] D. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.

[27] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology, Eurocrypt '93 Proceedings*, 1993.

# A Appendix: Error detection and correction

We describe here how we can estimate the error rate in the sifted set $S$ and then correct the discrepancies between Alice's and Bob's sifted keys using the interactive error-reconciliation scheme [27].

**Estimation of the error rate** The error rate in the sifted set can be estimated by comparing a small proportion of the bits chosen randomly in the sifted key. The compared bits should be encrypted with the one-time pad method so that a potential eavesdropper learns only the positions of the errors. A probabilistic property such as the Hoeffding inequality can be used to show that the observed error rate in the sampled proportion is not considerably lower than the error rate in the remaining part of the sifted set [13, 16, 23]. For asymptotic size of the sifted set, one can take arbitrarily small but positive proportion of the sifted key for this error rate estimation.

**Error correction** The remaining part of the sifted set that was not sampled in the previous step must be corrected. One-way linear error-correcting codes can be used for error correction. However, they are not very efficient and considerably higher number of redundant bits are required than the Shannon limit. A practical interactive correction scheme, devised by Brassard and Salvail [27] gets closer to this theoretical limit. A basic description of the scheme follows:

Alice and Bob group their bits into blocks of a given size, which has to be optimised as a function of the error rate. They exchange information about the parity of each block over the public channel. These parities should be encrypted using the one-time pad method. If their parities agree then they proceed to the next block. If their parities disagree, they deduce that there was an odd number of errors in the corresponding block, and search one of them recursively by cutting the block into two subblocks and comparing the parities of the first subblock: if the parities agree then the second subblock has an odd number of errors and if they do not, then the first subblock has an odd number of errors. Again, these parities should be encrypted. This procedure is continued recursively on the subblock with an odd number of errors. As a result of the encryption of the exchanged parities, a possible eavesdropper learns only the positions of the errors [7, 10].

After this first step, every considered block has either an even number of errors or none. Alice and Bob then shuffle the positions of their bits and repeat the same procedure with blocks of bigger size (this size being optimised as well). However, when an error is corrected, Alice and Bob might deduce that some blocks treated previously now have an odd number of errors. They choose the smallest block amongst them and correct one error recursively, as before. They proceed until every previously treated block has an even number of errors, or none.

Similar steps follow, and the interactive error correction terminates after a specified number of steps. This number is to be optimised in order to maximise the probability that no discrepancies remain and, at the same time, minimise the number of bits used for the one-time pad encryption. Readers are referred to the original paper [27] for precise description and treatment of this scheme.